[Windows XP / 7 / 8 / 10] File Execution (Open) Artifacts

Contact: junhyeong.lee@plainbit.co.kr, http://maj3sty.tistory.com

Information	Name	OS	Path	Comments
Execution Time **Target Volume Label** **Target Volume Serial Number** **Target File Size** **Target File Full Path** **Target Drive Type** **Local Mac Address**	Lnk	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- Recent: *%AppData%*\Microsoft\Windows\Recent*.lnk - MS Office: *%AppData%*\HNC\Office\Recent*.lnk - hwp: *%AppData%*\Microsoft\Office\Recent*.lnk	- Lnk 파일의 생성/수정/접근 시간의 연관성을 분석하면 최대 3개의 실행시간을 획득할 수 있음 (운영체제 버전 별 분석 방법 상이) - Target Drive Type과 Local Mac Address는 정확하지 않으므로 참고만 해야 함 - ID List의 Object ID를 활용해 파일의 동일성 입증 가능
Execution Time **Execution Application** **Target Volume Label** **Target Volume Serial Number** **Target File Size** **Target File Full Path** **Target Drive Type** **Local Mac Address**	Jumplist	Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%UserProfile%*\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDesctinations*.automaticDestinations-ms - *%UserProfile%*\AppData\Roaming\Microsoft\Windows\Recent\CustomDesctinations*.customDestinations-ms	- Target Drive Type과 Local Mac Address는 정확하지 않으므로 참고만 해야 함 - Execution Time 은 DestList의 LastRecord - Time이다.
Execution Time * (4 ~ 8) **Open File List** **Volume Serial Number**	Prefetch	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemRoot%*\Prefetch*.pf	- 프리패치가 존재했던 시스템이라면 반드시 복구 시도 - 프리패치 버전에 따라 실행 시간 개수가 다름 - Open File List는 프리패치 Reference List를 확인

				하면 됨
Malware Execution Time **Malware File Full Path** **Malware File Hash** **Malware Type(by behavior)** **Malware Threat Name**	Windows Defender – MP Log	Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%ProgramData%*\Microsoft\Windows Defender \Support\MPLog-<Date>-<Time>.log	- 행위 기반 탐지 로그가 기록되어 있어 알려져 있지 않은 악성코드도 의심 상태로 기록되어 있을 경우가 많음
Execution File Full Path	RecentFileCache	Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemRoot%*\AppCompat\Programs\ RecentFileCache.bcf	- 실행된 파일 경로와 순서만 파악 가능
Execution File Full Path **Execution Time** **Load Time on Memory**	Windows Error Reporting	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemDrive%*\ProgramData\Microsoft\WER\~*.wer - *%UserProfile%*\AppData\Local\Microsoft\Windows\ WER\~*.wer	
Execution File Full Path **Execution Time** **(Visit Time in History, Cache)**	Web Browser	Application dependent	- Browser record in history, Cache file	- file:// 프로토콜 항목
Service Name **Service Start/Stop Time** **(Event Generated Time)**	Event Log – Services	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemRoot%*\system32\winevt\Logs\System.evtx	- Event ID: 7034, 7035, 7036, 7040

Execution File Full Path **Execution Time** **(Event Generated Time)**	Event Log - Windows Error Reporting	Windows 2008 Windows 7	- *%SystemRoot%*\system32\winevt\Logs\Microsoft-Windows-WER-Diag%4Operational.evtx	- Event ID: 4
Malware Full Path **Malware Threat Name** **Malware Detection Time** **(Event Generated Time)** **Severity**	Event Log – Windows Defender	Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemRoot%*\system32\winevt\Logs\Microsoft-Windows-WindowsDefender%4Operational.evtx	- Event ID: 1117
Process ID **Process Image File Full Path** **Parent of Current Process** **Process Execution Time** **(Event Generated Time)** **Process Image File - Hash(SHA-1)** **Process Permission**	Event Log – Sysmon	Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemRoot%*\system32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx	- Sysmon 별도 설치 필요 - Event ID: 1
Execution File Full Path **Execution Time** **(Event Generated Time)**	Event Log – Program Telemetry	Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemRoot%*\system32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx	- Event ID: 500, 505
Execution File Full Path **Execution Time** **(Event Generated Time)**	Event Log – Program Compatibility Assistant	Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemRoot%*\system32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx	- Event ID: 17
Execution File Full Path **Execution Time** **(Event Generated Time)** **Execution User Name** **Execution Host Domain** **Parent of Execution File**	Event Log – Security Auditing	Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemRoot%*\system32\winevt\Logs\Security.evtx	- 로컬보안정책 => 로컬 정책 => 감사 정책 => “프로세스 추적 감사” 활성화 필요 - Event ID: 4688

Process ID **Execution File Name** **Execution Time** **Execution User Name** **Execution Host Domain** **Execution Command Line**	Event Log – Microsoft Windows Shell Core	Windows 10 Windows 2016	- *%SystemRoot%*\system32\winevt\Logs\Microsoft-Windows-Shell-Core%4Operational.evtx	- Event ID: 9707(시작), 9708(종료)
Execution File Full Path **Execution Count** **Execution Time** **(Key Last Written Time)** **Session ID**	Registry – UserAssist	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{<GUID>}\Count	- {CEBFF5CD~}: 실행 파일 실행 - {F4E57C4B~}: 바로가기 파일 실행 - ROT-13으로 인코딩 되어 있음 - 운영체제마다 실행 횟수 초기 값이 다름 - UserAssist key에 모든 실행 기록이 남는 것은 아님 (조건 존재)
Execution File Full Path **Execution File Size** **Execution Time** **Execution Complied Time** **Execution File Hash(SHA-1)**	Registry – AmCache	Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- *%SystemRoot%*\AppCompat\Programs\Amcache.hve	
Execution File Full Path **Execution File Size** **Execution Time** **Main Process Flag**	Registry – AppCompatCache	Windows XP Windows 2003 Windows Vista	- SYSTEM\ControlSet00#\Control\Session Manager\AppCompatibility	- 저장되어 있는 시간은 파일시스템 $SIA의 수정시간임, 실행시간이 아님
		Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- SYSTEM\ControlSet00#\Control\Session Manager\AppCompatCache	

Execution File Full Path **Execution Order** **Execution Time** **(Key Last Written Time)**	Registry – ComDlg32	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU	- 탐색기를 통해 실행된 파일 목록
Execution File Name **Execution Time** **(Key Last Written Time)**	Registry – Tracing	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- HKLM\SOFTWARE\Microsoft\Tracing\<Sub Key>	
Execution File Full Path	Registry – MuiCache	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- UsrClass.dat\Software\Classes\LocalSettings\MuiCache\<Sub Key>\<Sub Key>	- 마지막 Sub Key에 저장되어 있는 Value를 확인 해야 함
Execution File Full Path **Execution Time** **(Key Last Written Time)** **Execution Permission**	Registry – Services	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- HKLM\SYSTEM\ControlSet00#\Services\<Sub Key>	- SubKey의 Last Written Time은 서비스 의 처음 실행 시간으로 해석해야 함

Execution File Name **Execution Order**	Registry – RunMRU	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	- MRUList Value의 값을 보고 순서 파악
Lnk File Name **Execution Order**	Registry – RecentDocs	Windows XP Windows 2003 Windows Vista Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\<Sub Key>	- RecentDocs Key는 150개까지 기록 됨 - RecentDocs Sub Key는 확장자별로 MRUList가 존재함
Opened Folder Full Path **Folder Open Time** **(Key Last Written Time)** **Folder Created Time** **Folder Modified Time** **Folder Accessed Time** **File Reference Information** **- NTFS: $MFT Entry #, Seq #** **- FAT: Directory Entry #** **- exFAT: Null** **Ref) FTP Server Directory-List, HTTP and FTP URIs, ZIP file contents**	Registry – Shell Bags	Windows XP Windows 2003 Windows Vista	- NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags - NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU - NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bags - NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\BagMRU	- 폴더의 생성/수정/접근 시간은 NTFS $SIA 시간임 - 폴더의 생성/수정/접근 시간은 NTFS 경우 UTC+0으로 저장되고, FAT 경우 Local Timezone을 상속 받음
		Windows 2008 Windows 7 Windows 8 Windows 10 Windows 2012	- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags - USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU - NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU - NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags	

Execution File Full Path **Execution Start Time** **Execution End Time** **Execution Expire Time** **Execution File Modified Time** **Parent of Execution File**	Timeline (Activity Log)	Windows 10	- *%UserProfile%*\AppData\Local\ConnectedDevicesPlatform\L.<User Name>\ActivitiesCache.db	- JSON 데이터 중 'application' Key의 AppID는 Parent App을 의미 함 - Windows RS4에서 새로 추가 됨 - 파일뿐만 아니라 인터넷 활동 기록도 파악할 수 있음